

**REMARKS**

This communication is responsive to the Office Action dated 13 July 2007, as extended by payment of appropriate extension of time fees pursuant to 37 CFR § 1.136(a).

Claims 1-6, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-36, 38, 40-44 and 46-56 were pending prior to this paper. In this paper, the Applicant has:

- cancelled claims 5, 6, 47 and 51;
- amended claims 1, 4, 11, 25, 41, 46, 48 and 52; and
- added new claims 57-58.

The Applicant submits that the amendments to claims 1, 4, 11, 25, 41, 46, 48 and 52 and new claims 57 and 58 are completely supported by the application as originally filed and add no new matter.

Claims 1-4, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-36, 38, 40-44, 46, 47-50 and 52-58 are pending after this amendment.

**Claims 1-3, 17, 18, 20, 25, 27, 34-36, 38, 40-42, 48-50 and 55**

The Examiner has raised the combination of US6,052,780 (Glover), US6,892,306 (En-Seung et al.) and US 2001/0011238 (Eberhard et al.) in connection with claim 1. The Applicant submits that claim 1 (as amended) patentably distinguishes the combination of Glover, En-Seung et al. and Eberhard et al.

Following the Examiner' logic presented on pages 4-6 of the Office Action, the Examiner correctly acknowledges that Glover fails to teach or suggest the claim 1 feature of "receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key".

The Examiner appears to express the view that En-Seung et al. disclose the claim 1 feature of receiving a decryption key (temporary validation key) from a remote server at a user computing device, the decryption key itself encrypted at the remote server with a user key (user's key), such that the user computing device can use the user key to decrypt the decryption key. The Examiner contends further that it would be obvious for a person skilled in the art to combine this feature of En-Seung et al. with the content delivery system disclosed by Glover. However, the Examiner correctly acknowledges that neither Glover nor En-Seung et al. teach or suggest the claim 1 feature of "the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device."

The Examiner appears to express the view that this claim 1 feature ("the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device") is disclosed by Eberhard et al. The Examiner contends further that it would be obvious for a person skilled in the art to combine this aspect of the Eberhard et al. system with the features of Glover and En-Seung et al. to arrive at the claim 1 features.

The Applicant has amended claim 1 to more particularly recite that the decryption key is "received from the remote server at the user computing device over a communication network" and to incorporate features substantially similar to those recited in previously pending claim 47. More specifically, claim 1 now recites that receiving the (media) file at the user computing device comprises "receiving the file from a remote computer over the communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received." This claim 1 feature specifies that the encrypted media file and the decryption key are received over a single communication network but from different computers and over different communication paths. The Applicant submits that the combination of Glover, En-seung et al. and Eberhard et al. fails to teach or suggest this feature.

Glover

Glover teaches that encrypted media content may be purchased separately (e.g. on a DVD) and that a "decryption key" may then be received from a "content provider" when the user calls a toll-free telephone number - (col. 21, ln. 20-65). This aspect of Glover does not amount to receiving a media file and a decryption key over a single communication network from two different computers as recited in claim 1. Glover also teaches a so called "on-line" embodiment where the media content and the "decryption key" are both downloaded from a "service provider" - (col. 22, ln. 1-20). Glover specifically discloses that the decryption "algorithms are downloaded at the time of recording from a service provider" (col. 22, ln. 12-13) and that the encrypted media content is provided to the service provider "to present to their customers" (col. 22, ln. 14-15). In the Glover "on-line" embodiment, the "service provider" provides end users with both the encrypted content and the decryption algorithms. In direct contrast, claim 1 (as amended) recites that the (media) file and decryption key are received over the same communication network but from different computers (i.e. media file is received over the communication network "from a remote computer" and decryption key is received over the network "from a remote server"). Moreover, claim 1 recites that the (media) file is received through a communication path that does not include the server from which the decryption key is received.

Accordingly, Glover fails to teach or suggest that the media content and the decryption key are received over a single communication network from two different computers and over two different communications paths as recited in claim 1.

En-Seung et al.

En-Seung et al. describe a content delivery system wherein both "digital information" (e.g. media content) and a "temporary validation key" (alleged by the Examiner to have the characteristics of the claim 1 "decryption key") are received at a user "terminal unit" 10/20 from the same "service server" 12/22.

Figures 1-4 depict various embodiments of the En-Seung et al. content delivery system and clearly show (e.g. by way of non-enumerated arrows) that the only component in

communication with the user "terminal unit" is a "service server" (see terminal unit 10 and service server 12 in Figures 1 and 2 and terminal unit 20 and service server 22 in Figures 3 and 4). Figures 1-4 of En-Seung et al. clearly show that all components of the En-Seung et al. system communicate with terminal unit 10/20 through service server 12/22. Accordingly, En-Seung et al. explicitly disclose that the communication path through which encrypted files and the decryption key are received at terminal unit 10/20 includes service server 12/22. In direct contrast, claim 1 (as amended) recites that the (media) file is received through a communication path that does not include the server from which the decryption key is received.

Figures 1 and 2 of En-Seung et al. are described at col. 6, ln. 18-col. 7, ln. 31. This passage from En-Seung et al. describes how service server 12 generates a header which includes a "temporary validation key" - (col 6, ln. 30-32). En-seung et al. also describe how service server 12 combines the "temporary validation key" with encrypted "digital information" to form a protocol for copyright protection which is "transmitted to the user's terminal unit 10" - (col. 6, ln. 32-36). The En-Seung et al. "temporary validation key" is alleged by the Examiner to exhibit the features of the claim 1 "decryption key". The En-Seung et al. "digital information" includes media content - (col. 4, ln. 47-49). Accordingly, the portion of En-Seung et al. describing Figures 1 and 2 specifically teaches that both the media content and the decryption key are received at the user computing device from the same "service server" 12.

Figures 3 and 4 of En-Seung et al. are described at col. 7, ln. 32-67. This passage from En-Seung et al. states that "[s]ervice server 22 generates a temporary validation key" - (col. 7, ln. 52-54). En-Seung et al. also states that "[s]ervice server 22 adds the digital information ... to form the copyright protection protocol and then transmits the copyright protection protocol to terminal unit 20" - (col. 7, ln. 56-61). The En-Seung et al. "temporary validation key" is alleged by the Examiner to have the characteristics of the claim 1 "decryption key". The "digital information" referred to by En-Seung et al. includes media content - (col. 4, ln. 47-49). Accordingly, the portion of En-Seung et al. describing Figures 3 and 4 specifically teaches that both the decryption key and the media content are received from the same "service server" 22.

Accordingly, the written description of En-Seung et al. contrasts directly with claim 1 which recites that the (media) file and decryption key are received over the same communication network but from different computers (i.e. media file is received over the communication network "from a remote computer" and decryption key is received over the network "from a remote server") and over different communication paths.

Based on this reasoning, En-Seung et al. fail to teach or suggest the claim 1 feature that the media content and the decryption key are received over a single communication network from two different computers over two different communications paths.

*Eberhard et al.*

Eberhard et al. disclose a system for delivery of electronic books. Eberhard et al. disclose the user of a single encryption key which is generated at the user machine and then transmitted (via a retailer server and an authentication server) to a content provider (publisher server) which encrypts the electronic book with the encryption key before downloading the electronic book to a user - (paragraphs [0023]-[0026]). The Eberhard et al. decryption key is generated locally at the user machine. Eberhard et al. do not teach or suggest the claim 1 feature of receiving a media file and a decryption key over a single communication network from two different computers over two different communication paths.

The Eberhard et al. system is shown best in Figure 1. As pointed out by the Examiner, the Eberhard et al. encryption key is described in paragraph [0023], which states "reader 115 is typically identified by unique indicia such as a serial number 117 and in a typical embodiment also includes a private encryption key 119 which may be uniquely associated with either a specific reader or a specific customer." Paragraph [0023] also describes how user PC 110 includes software (e.g. a Java applet or helper application) 125 which interrogates reader 115 to obtain the serial number of other customer ID 117. These aspects of Eberhard et al. clearly explain how the Eberhard et al. serial number/encryption key/customer ID 117 is generated local to reader 115/user PC 110. In direct contrast to this aspect of Eberhard et al., claim 1 recites a "decryption key" that is received at the user computing device from a remote server

"over a communication network" - i.e. the same communication network through which the (media) file is received at the user computing device.

Eberhard et al. describe how electronic books (i.e. media content files) are downloaded from a publisher server 100 to user PC 110 and to reader 115 over a web browser based communication network - (paragraph [0026]). However, this aspect of Eberhard et al. does not disclose the claim 1 feature of receiving the (media) file at the user computing device "from a remote computer over the communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received", because the Eberhard et al. serial number/encryption key/customer ID 117 is generated locally to reader 115/user PC 110 and is not received from a remote server over the same communication network through which the media file is received.

Accordingly, Eberhard et al. do not teach or suggest the claim 1 feature of receiving decryption key and a file containing media content over a single communication network but from two different computers over two different communication paths.

*Conclusions with respect to claims 1-3, 17, 18, 20, 25, 27, 34-36, 38, 40-42, 48-50 and 55*

Claim (1 as amended) recites "wherein receiving the file at the user computing device comprises receiving the file from a remote computer over a communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received." This claim 1 feature specifies that the encrypted media and the decryption key are received over a single communication network but from different computers over two different communication paths. The Applicant submits that the combination of Glover, En-seung et al. and Eberhard et al. fails to teach or suggest this claim 1 feature.

This claim 1 feature provides unique advantages to the Applicant's system. More particularly, a content provider is able to widely release encrypted media content without having to be concerned about the encrypted media content being shared among end users. In accordance

with the Applicant's system, end users can share encrypted media content with one another (i.e. end users do not have to download the encrypted content from a central server). This allows end users to take advantage of popular peer to peer networks (as more particularly recited in claims 25, 41 and 48-50, for example). Even though encrypted media files can be shared between end users, the end users must still obtain a decryption key from the content provider. Since decryption keys are much smaller (in terms of memory) than media content, the Applicant's system saves bandwidth usage for content providers, as only decryption keys are required to be obtained from a central server. Copyright protection is maintained because each decryption key obtained from the content provider is encrypted with a user key that is based on one or more characteristics of the end user's computing device. Thus, a separate user key is used for each user computing device on which it is desired to play back the media content.

Based on the reasoning presented above, the Applicant submits that claim 1 (as amended) patentably distinguishes the combination of Glover, En-Seung et al. and Eberhard et al. Claims 2, 3, 17, 18, 20, 25, 27, 34-36, 38, 40-42, 48-50 and 55 depend from claim 1 and are submitted to patentably distinguish the prior art of record for at least this reason.

#### **Claims 4, 11, 21, 28, 31, 33, 43, 44, 52-54 and 56**

The Examiner has raised the combination of Glover, En-Seung et al., US 6,564,248 (Budge et al.) and Eberhard et al. in connection with claim 4. The Applicant submits that claim 4 patentably distinguishes the combination of Glover, En-Seung et al., Budge et al. and Eberhard et al.

Applicant has amended claim 4 in a manner similar to that of claim 1 to more particularly recite that the decryption key is obtained from a remote server "over a communication network" and to incorporate features substantially similar to those recited in previously pending claims 5 and 51. More specifically, claim 4 now recites "wherein receiving the single file comprises downloading said single file from a computer via the communication network; wherein the communication network from which the single file is downloaded includes the remote server from which the decryption key is obtained; and wherein downloading the single

file from the computer via the communication network comprises downloading the single file from the computer through a communication path that does not include the remote server from which the decryption key is obtained." This claim 4 feature specifies that the encrypted media file and the decryption key are received over a single communication network but from different computers over different communication paths. The Applicant submits that the combination of Glover, Budge et al., En-Seung et al. and Eberhard et al. fails to teach or suggest this feature.

As discussed above in relation to claim 1, Glover, En-Seung et al. and Eberhard et al. do not disclose receiving a decryption key and a (media) file over the same communication network but from different computers and over different communication paths as recited in claim 4. The addition of Budge et al. fails to remedy this deficiency.

Based on this reasoning, the Applicant submits that claim 4 (as amended) patentably distinguishes the combination of Glover, Budge et al., En-Seung et al. and Eberhard. Claims 11, 21, 28, 31, 33, 43, 44, 52-54 and 56 depend from claim 4 and are submitted to patentably distinguish the prior art of record for at least this reason.

#### **Claim 46**

The Examiner has raised the combination of Glover, En-Seung et al. and Eberhard et al. in connection with claim 46. The Applicant submits that claim 46 (as amended) patentably distinguishes the combination of Glover, En-Seung et al. and Eberhard et al.

The Applicant has amended claim 46 to more particularly recite that the decryption key is "received from the remote server at the user computing device over a communication network" and to incorporate features substantially similar to those recited in previously pending claim 47. More specifically, claim 46 now recites that receiving the (media) file at the user computing device comprises "receiving the file from a remote computer over the communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received." This claim 46 feature specifies that the encrypted media file

and the decryption key are received over a single communication network but from different computers and over different communication paths.

As discussed above in relation to claim 1, Glover, En-seung et al. and Eberhard et al. do not teach or suggest receiving a decryption key and a (media) file over the same communication network but from different computers and over different communication paths as recited in claim 46. The Applicant submits therefore that claim 46 patentably distinguishes the combination of Glover, En-Seung et al. and Eberhard et al.

**Additional comments relating to claims 48-50**

The Examiner has raised the combination of Glover, En-Seung et al. and Eberhard et al. in connection with claim 48. The Applicant submits that claim 48 patentably distinguishes the cited references.

Claim 48 incorporates features that describe sharing an encrypted media file between end users. These features contrast directly with the content delivery systems disclosed by Glover, En-Seung et al. and Eberhard et al., which require content to be independently obtained by each end user from a centralized server. More particularly, claim 48 recites sending the (media) file "from the user computing device to a second user computing device over the communication network over a second communication path that does not include the remote server" and then, at the second user computing device, repeating steps similar to those recited in claim 1 to request and receive a decryption key encrypted with a user key from the remote server and to decrypt the media content.

This claim 48 combination of features is not disclosed by the cited references. More particularly, the cited references do not teach or suggest sharing (media) files between end user computers where the media files are decrypted to playback the media content. In contrast, each of the cited references teach separately obtaining media files at each user computer from a central server.

Glover

As discussed above, Glover describes an "on line" embodiment where each user corresponds with the "service provider" to obtain both the media content and the encryption information. Glover does not teach or disclose that encrypted media files are sent between users and that each user then accesses decryption information from the same centralized "remote server". Accordingly, Glover fails to disclose the claim 48 feature of sending the (media) file "from the user computing device to a second user computing device over the communication network over a second communication path that does not include the remote server" and then repeating the decryption process at the second user computing device.

En-Seung et al.

As discussed above, En-Seung et al. disclose that both the digital information (e.g. a media file) and the temporary validation key (alleged to be the claim 1 decryption key) originate from central service servers 12/22 and are sent from the central service servers 12/22 to user terminal units 10/20 - (Figures 1-4). En-Seung et al. do not disclose how digital information can be transferred between user terminal units 10/20.

The Examiner expresses the view that En-Seung et al. disclose the features of claim 48 at col. 3, ln. 5-18, col. 6, ln. 30-36 and col. 7, ln. 6-16 and 52-61. The Applicant respectfully submits that this view is incorrect. None of these passages from En-Seung et al. disclose or suggest that media files are transferred between user computing devices. Neither these passages nor any other part of En-Seung et al. teach the claim 48 combination sending the (media) file "from the user computing device to a second user computing device over the communication network over a second communication path that does not include the remote server" and then repeating the decryption process at the second user computing device.

In addition to the above-described differences, claim 48 recites, after receiving the (media) file at the second user computing device, "receiving the decryption key from the remote server at the second user computing device ... and decrypting the media content at the second user computing device using the integral decryption engine and the decryption key". The use of the definite article "the" to describe "the decryption key" in claim 48 implies that the decryption

key received at the second user computing device is the same as the decryption key received at the first user computing device. The En-Seung et al. system does not support the use of one "decryption key" that can be used by multiple users on different computers at the same or different times. The Examiner alleges that the "decryption key" recited in claims 1 and 48 is akin to the En-Seung et al. "temporary validation key". En-Seung et al. specifically teach that the temporary validation key remains "valid only while the user is in the process of accessing the system, that is temporarily" (col. 5, ln. 40-42) and that temporary validation keys are different depending on the time that a user accesses the system (col. 5, ln. 38-40). This aspect of En-Seung et al. teaches directly away from the claim 48 feature of using the same decryption key at two different user computing devices.

*Eberhard et al.*

As discussed above, Eberhard et al. describe a system where electronic books (in an encrypted format) are downloaded from a "publisher server" 100. The electronic books are encrypted in a format that is particular to each end user reader 15 based on communication of a serial number/encryption key/customer ID 117 to publisher server 100 (via retailer server 120 and authentication server 135). In order to obtain the media content, each user must separately send serial number/encryption key/customer ID 117 to publisher server 100 (via retailer server 120 and authentication server 135) and then download the electronic book from publisher server 100. Eberhard et al. do not teach or disclose that (media) files are sent between users and that each user then accesses decryption information from the same centralized "remote server". Accordingly, Eberhard et al. fail to disclose the claim 48 feature of sending the (media) file "from the user computing device to a second user computing device" over the communication network over a second communication path that does not include the remote server" and then repeating the decryption process at the second user computing device.

*Conclusions with respect to claims 48-50*

Based on the reasoning presented above, the Applicant submits that claim 48 patentably distinguishes the combination of Glover, En-Seung et al. and Eberhard et al. Claims 49 and 50 depend from claim 48 and are submitted to be patentable over the cited references for at least this reason.

**Additional comments relating to claims 52-54**

The Examiner has raised the combination of Glover, Budge et al. En-Seung et al. and Eberhard et al. in connection with claim 52. The Applicant submits that claim 52 patentably distinguishes the cited references.

Claim 52 incorporates features that are similar to those of claim 48 discussed above and describe sharing an encrypted media file between end users. These features contrast directly with the content delivery systems disclosed by Glover, En-Seung et al. and Eberhard et al., which require content to be independently obtained by each end user from a centralized server. More particularly, claim 52 recites sending the (media) file "from the user computing device to a second user computing device over the communication network over a second communication path that does not include the remote server" and then, at the second user computing device, repeating steps similar to those recited in claim 4 to request and receive a decryption key encrypted with a user key from the remote server and to decrypt the media content.

As discussed above, this claim 52 combination of features is not disclosed by Glover, En-Seung et al. or Eberhard et al. More particularly, these references do not teach or suggest sharing (media) files between end user computers where the media files are decrypted to playback the media content. In contrast, each of the cited references teach separately obtaining media files at each user computer from a central server. Budge et al. fail to remedy this deficiency.

Based on this reasoning, the Applicant submits that claim 52 patentably distinguishes the combination of Glover, Budge et al., En-Seung et al. and Eberhard et al. Claims 53 and 54 depend from claim 52 and are submitted to be patentable over the cited references for at least this reason.

**Claims 57 and 58**

The Applicant has added new claims 57 and 58 for which patent protection is sought. New claims 57 and 58 are submitted to be completely supported by the application as originally filed and to add no new matter.

Claims 57 and 58 depend respectfully from claims 1 and 4 and are submitted to be allowable over the prior art of record for at least this reason. Claims 57 and 58 also recite features which are submitted to further distinguish the cited references. More particularly, none of the cited references teach or suggest that a user key that is based on a "digital fingerprint" of the user computing device.

**Conclusions**

In view of the foregoing amendments and arguments, the Applicant respectfully submits that this application is now in condition for allowance and requests reconsideration and allowance of this application.

Respectfully submitted,  
OYEN WIGGS GREEN & MUTALA

By:

  
Todd A. Rattray  
Registration No. 60,483  
Vancouver, Canada  
tel: 604.669.3432  
fax: 604.681.4081  
e-mail: TARDOcket@patentable.com